

Encryption and Tokenization of Card Security using Cryptographic Algorithms

Prof. Geethalakshmi N M, Arun Kumar T O, Tushara N, Varsha A, Vijetha K S

PROFESSOR & STUDENTS OF DEPARTMENT INFORMATION SCIENCE AND
ENGINEERING

ACHARYA INSTITUTE OF TECHNOLOGY, SOLADEVANAHALLI. 560107

Abstract: There are several alternative strategies that can be used when utilising cryptography to encrypt card information. Encryption's main objective in this situation is to prevent sensitive card information from being intercepted and used fraudulently, including the card number, expiration date, and security code.

Using SSL (Secure Socket Layer) or TLS (Transport Layer Security), which establishes a safe, encrypted connection between a website or app and the server where the card information is stored, is one popular method of encrypting card information. This is frequently used for online transactions, such as when paying with a mobile app or buying something from an e-commerce website.

Using end-to-end encryption is an alternative strategy that guarantees that card information is encrypted from the time it is entered into a device, website, or app until it reaches its destination. This is frequently used with tokenization, which exchanges the sensitive card information for a singular token that can be safely kept and used for upcoming transactions without disclosing the actual card data.

Additionally, a number of cryptographic protocols and algorithms, including AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography), can be used to encrypt card information. These algorithms and protocols jumble the data using intricate mathematical computations so that it cannot be decoded without the right decryption key.

1.INTRODUCTION

A crucial component of contemporary payment systems that guarantees the security and privacy of sensitive financial information is the encryption of card data using cryptography. Utilising mathematical methods and protocols to secure data against unauthorised access or change is known as cryptography.

When it comes to card data, encryption entails putting the private information into an unreadable format that can only be unlocked with the right key or password. With the encryption key missing, the data is rendered worthless even if it is intercepted by a third party thanks to this measure.

The confidentiality and integrity of the data are all protected during transmission and storage using a

variety of methods, including as SSL/TLS, end-to-end encryption, and tokenization.

To avoid fraud, identity theft, and other security breaches that may have detrimental financial and legal repercussions, cardholder data must be encrypted. As a result, it is essential to protect payment systems and a major worry for both customers and businesses, as well as financial institutions.

2.EXISTING SYSTEM AND ITS PROBLEM

Numerous systems currently in use encrypt card data using encryption, including:

- The international payment card standard known as EMV (Europay, Mastercard, and Visa) employs chip technology and cryptographic methods to safeguard transactions. It is widely used throughout the rest of the world, including Europe, Asia, and the United States, where adoption is progressing gradually. The EMV system's ability to make it harder for fraudsters to produce fake cards is one of its main advantages.
- Payment Card Industry Data Security Standard (PCI DSS): These security guidelines were developed by the major credit card firms to assist combat fraud and guarantee the safe handling of cardholder data. It includes, among other things, specifications for network security, access controls, and encryption.

- Some credit card companies utilise the 3D Secure protocol to give an extra degree of authentication to online transactions. By using cryptographic methods to confirm the cardholder's identity, it can assist stop fraudulent transactions.

Despite the obvious advantages of these systems, utilising cryptography to encrypt card information can nevertheless lead to some issues. Here are a few illustrations:

- Key management: To secure data, cryptography uses encryption keys, and keeping track of these keys can be difficult and complicated. If keys are not properly managed, they may be mishandled, stolen, or lost, which could jeopardise the system's security.
- Implementation mistakes: If cryptographic algorithms are not implemented correctly, even the most secure ones may be subject to attack. When encryption systems are implemented incorrectly, vulnerabilities might develop that an attacker could take advantage of.
- Encryption is sometimes ineffective against internal threats, despite its ability to protect against exterior threats. Even

if critical card information is encrypted, employees who have access to it run the risk of misusing it for their own gain.

In general, it is crucial to understand that encryption utilising cryptography is not a foolproof method for protecting card information. For the best possible defence against fraud and other security concerns, it must be used in conjunction with other security measures like access limits and monitoring.

3.RELATED WORK

A crucial part of contemporary payment systems is the encryption of card data using cryptography, and work in this area is still ongoing. A few instances of the work being done are as follows:

- **Secure key management:** Managing the keys that are used to encrypt and decrypt the data is one of the difficulties with encryption. In order to handle these keys more effectively and securely, researchers are creating cloud-based key management services or hardware-based security modules (HSMs).
- **Post-Quantum Cryptography:** With the development of quantum computers, established encryption techniques like RSA and ECC may be subject to

intrusion. Post-quantum cryptography, which involves creating new cryptographic algorithms immune to quantum assaults, is currently being researched.

- **Homomorphic Encryption:** This type of encryption enables calculations to be made on encrypted material without first having to decrypt it. When sensitive data needs to be processed or analysed while still retaining its privacy, this could be helpful.
- **Multi-Party Computation:** This method enables several parties to collaboratively compute a function on their inputs without disclosing their individual inputs to one another. When sensitive data needs to be processed by several parties while retaining its privacy, this could be employed.
- **Blockchain-based Payment Systems:** Blockchain technology can be used to develop safe, decentralised, and open payment systems. Researchers are looking into new encryption methods as well as the use of blockchain for payment systems.

The current research into employing cryptography to encrypt credit card data is

primarily focused on enhancing payment systems' security, effectiveness, and privacy.

4.OVERVIEW OF PROPOSED SYSTEM

As an AI language model, I do not have access to any particular project or planned system, but I can give a broad picture of how cards are encrypted in a system employing cryptography.

The following elements would most likely be included in a typical proposed system for employing cryptography to encrypt card information:

- An encrypted means of collecting and sending card data, such as SSL/TLS or end-to-end encryption, as well as secure storage and transmission protocols, may be used.
- A technique for encrypting card data would entail picking the right cryptographic algorithm or protocol, like AES, RSA, or ECC, then securely implementing it within the system.
- An effective key management system would ensure that only authorised users have access to the encryption and decryption keys by using secure key storage techniques, strong password policies, and access controls.

- A technique for safely storing and sending the encrypted card data - Tokenization or other secure data storage techniques, along with secure transmission protocols, may be used to guarantee that the encrypted card data is safe both during transmission and storage.
- Implementing a decryption algorithm or protocol that can correctly decrypt the encrypted card information using the right key would be a secure way to decrypt the card data.

The use of certain cryptographic algorithms and protocols, the key management system, and the safe transmission and storage of the encrypted data are just a few of the variables that would need to be taken into account in a suggested system for employing cryptography to encrypt card information. A system can offer good protection for card information and aid in preventing fraud and identity theft by properly integrating these components.

5.PERFORMANCE EVALUATION

With the development of technology and algorithms, card encryption performance has changed dramatically over time, resulting in more efficient and safe encryption techniques.

Early on, symmetric-key techniques like DES (Data Encryption Standard) and 3DES (Triple Data Encryption Standard) were frequently used for

encryption in electronic payment systems. These algorithms offered a fundamental level of security, but they were slow and susceptible to some assaults.

Asymmetric-key algorithms with higher levels of security and efficiency, like RSA, gained popularity as processing power rose. These techniques encrypt data using a public key, and the recipient's private key is required to decrypt it. This method is quicker than symmetric-key algorithms and offers a higher level of security.

Modern symmetric-key algorithms like AES, which are quicker and more secure than older symmetric-key algorithms, have gained popularity in recent years. AES is now the industry standard for encrypting credit card data and is utilised in several applications, including mobile payments, internet transactions, and point-of-sale systems.

Algorithm improvements have been accompanied by a rise in the use of hardware encryption. Software-based encryption can sometimes be slower and less secure than hardware encryption, which uses specialised processors to carry out encryption and decryption procedures.

Overall, the desire for greater security and better performance has driven the growth of card encryption utilising cryptography. We can anticipate future advancements in encryption methods and algorithms, as well as brand-new hardware-based methods of encryption, as technology develops.

6.RESULT ANALYSIS

Using cryptography to encrypt credit card data has a number of significant advantages and outcomes:

- **Enhanced security:** When card data is encrypted using cryptography, it becomes much harder for thieves to intercept and steal important information, like credit card numbers or personal data. This aids in the prevention of fraud, identity theft, and other online crimes.
- **Regulation adherence:** Strict data security rules, such as the Payment Card Industry Data Security Standard (PCI DSS), apply to many businesses. Organisations can comply with these requirements and avoid exorbitant fines and penalties by encrypting card information using encryption.
- **Customers are more inclined to trust a company** with their sensitive data if they are confident that their card information is encrypted and kept secure. This could improve client happiness and brand loyalty.
- **Reduced liability:** Organisations can lessen their exposure in the event of a data breach by encrypting card information using cryptography. Encrypting sensitive data may prevent it from being viewed as "compromised" by authorities or the general public, hence reducing the risk of legal liability and reputational harm.

Overall, modern payment systems and cybersecurity practises depend heavily on the encryption of card information utilising cryptography. Organisations may

considerably lower the risk of data breaches and cyberattacks while also enhancing consumer trust and regulatory compliance by deploying robust encryption protocols and algorithms.

7. PERFORMANCE ANALYSIS

There are a number of variables to take into account while evaluating the effectiveness of card data encryption utilising cryptography, including speed, security, and scalability.

- **Speed:** The speed of encryption and decryption is a crucial factor. The computational complexity of encryption techniques can result in longer processing times and possibly longer transaction times. However, contemporary encryption methods like AES and ECC are made to be quick and effective, minimising any impact on speed.
- **Security:** The degree of security offered by the encryption algorithm is a crucial additional consideration. The algorithm must be safe enough to prevent unauthorised access to or interception of the card data. For instance, AES is frequently used in numerous applications, including the encryption of credit card information, and is thought to be quite secure. It's crucial to remember that an encryption technique's security is dependent on a variety of elements, including the size of the encryption key, the calibre of the random number generator used to create the key, and the robustness of the algorithm itself.

- **Scalability:** The scalability of the encryption technique is another crucial factor, especially in systems that perform a lot of transactions. Due to speed concerns and potential security flaws, some encryption methods may not be able to handle massive amounts of data. However, contemporary encryption techniques like AES and ECC are built to handle massive amounts of data without sacrificing security or performance.

In conclusion, utilising cryptography to encrypt card data can be a good technique to safeguard sensitive information from being accessed by unauthorised people. Modern encryption algorithms are built to be efficient and scalable while delivering a high level of security to guard against fraud and identity theft, even if there may be some performance effect associated with encryption.

8. FUTURE WORK

Although cryptographic encryption of card data has advanced significantly in recent years, there is always space for advancement. The following could be some future research in this field:

- **Post-quantum cryptography:** As quantum computers continue to advance, there is a rising demand for post-quantum encryption, which can fend off attacks from these devices. This can entail creating new encryption algorithms that

are resistant to quantum assaults or modernising current methods to make them so.

- **Homomorphic encryption:** Homomorphic encryption enables computations to be conducted on encrypted data without disclosing the underlying information. Data can be encrypted while still being processed. Due to the fact that it would enable transactions to be conducted without disclosing sensitive data, this might be especially helpful for card information.
- **Multi-party computation** entails several people working together to compute a function while maintaining the confidentiality of their inputs. This might be applied to card transactions to enable group collaboration without disclosing private information and lower the danger of data breaches.
- **Solutions built on the blockchain:** Blockchain technology has the power to completely change how card data is processed and stored. Blockchain-based solutions might offer a more secure and open approach to manage card information by using a decentralised ledger, lowering the risk of fraud and boosting confidence in the payment system.
- **Machine learning-based solutions:** By examining trends in card data, machine learning algorithms can be used to identify and stop fraudulent transactions. These algorithms may become increasingly more successful at identifying fraud and safeguarding card

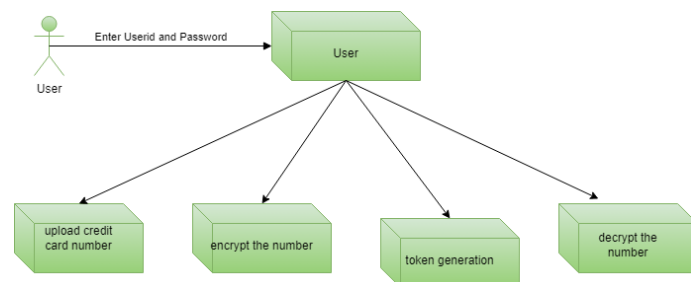
information as machine learning techniques advance.

9.CONCLUSION

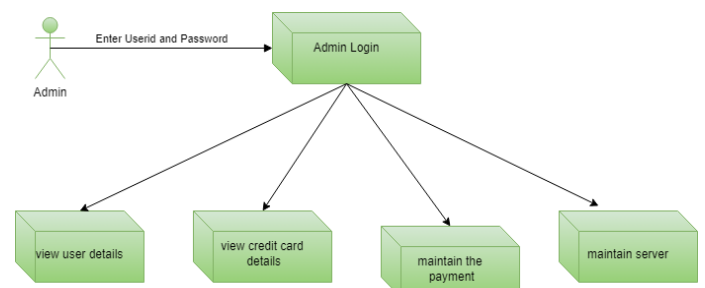
In conclusion, utilising cryptography to encrypt card data is crucial for preventing sensitive information from being intercepted and utilised fraudulently. Cardholder data can be protected during transactions using a variety of encryption techniques, including SSL/TLS, end-to-end encryption, tokenization, and cryptographic algorithms like AES, RSA, and ECC.

10.SNAPSHOTS

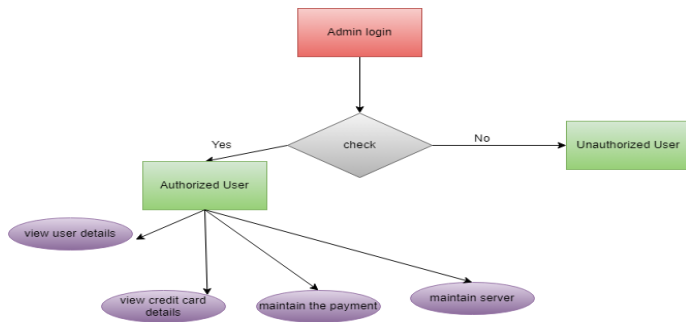
1. System Architecture for Admin



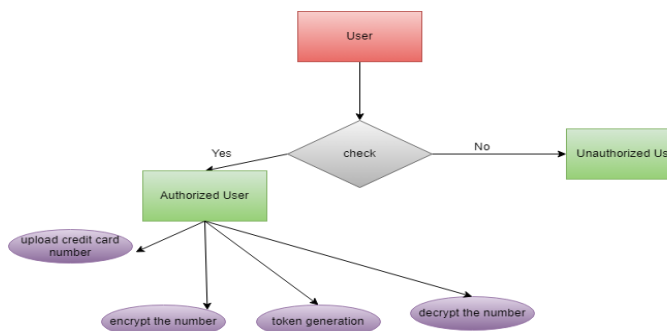
2. System Architecture for User



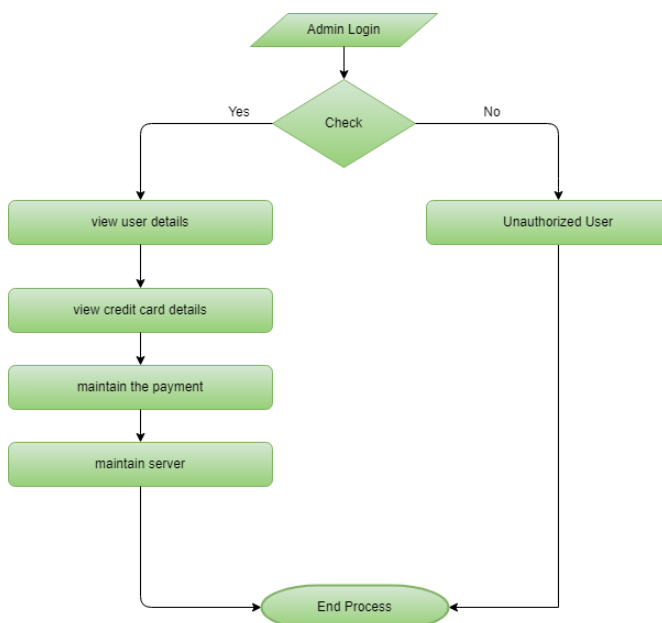
3. Flow Chart for Admin



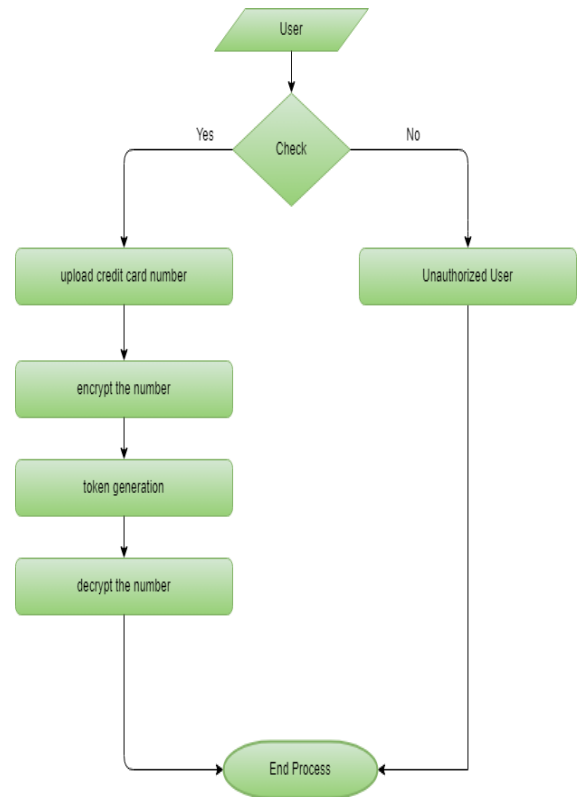
4. Flow Chart for User



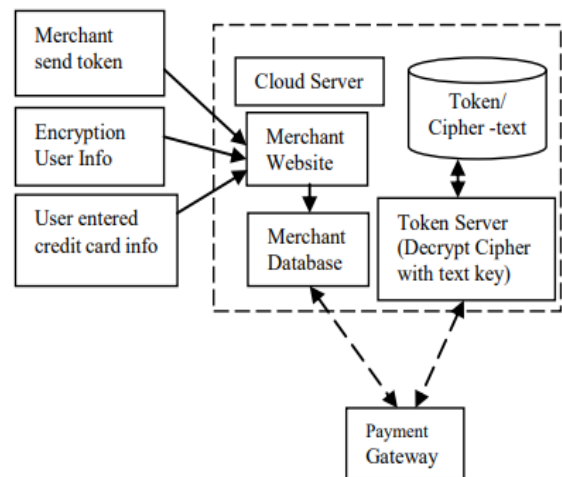
5. Data Flow Diagram for Admin



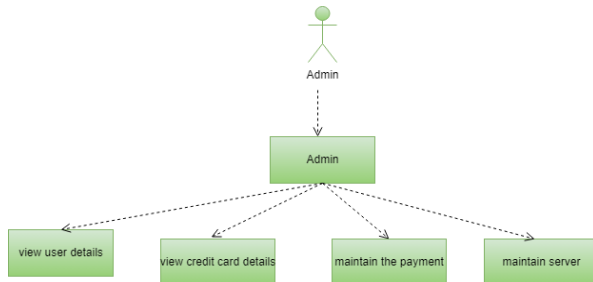
6. Data Flow Diagram for User



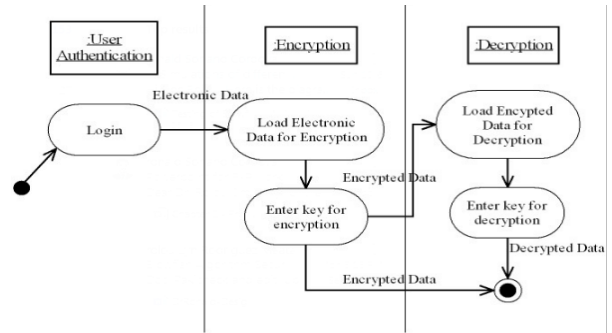
7. Class /Object Diagram



8. Use Case Diagram for Admin

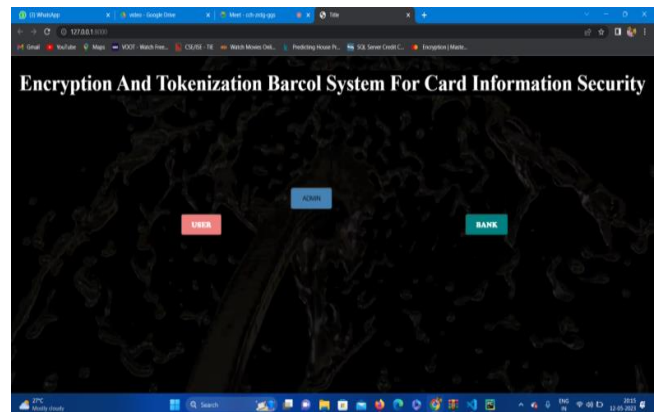
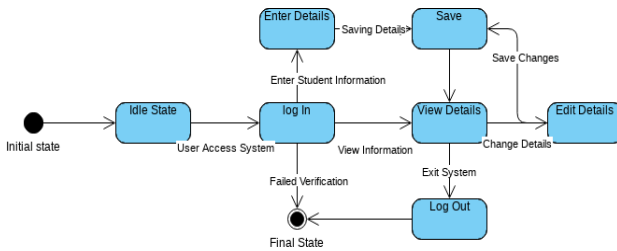


12. Activity Diagram

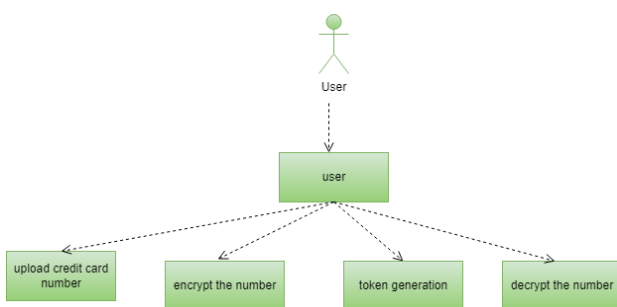


13. Introduction Page

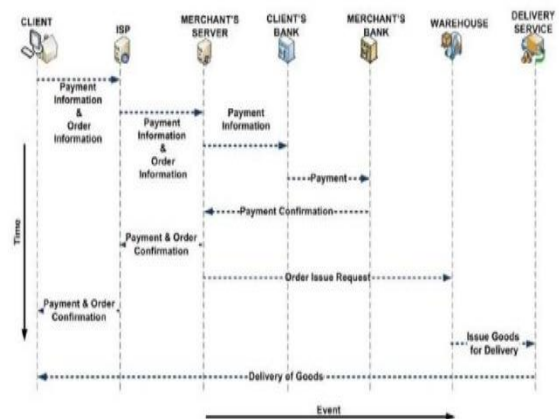
11. State Chart Diagram



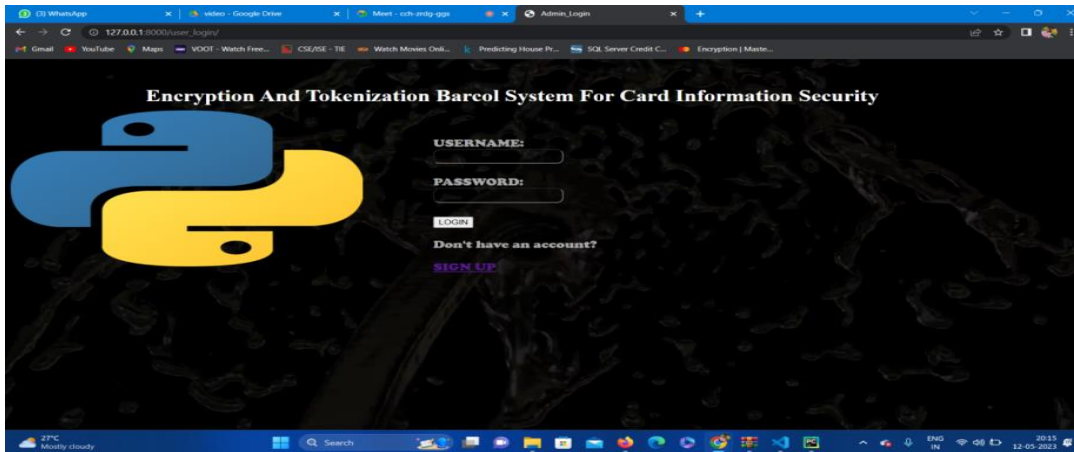
9. Use case Diagram for User



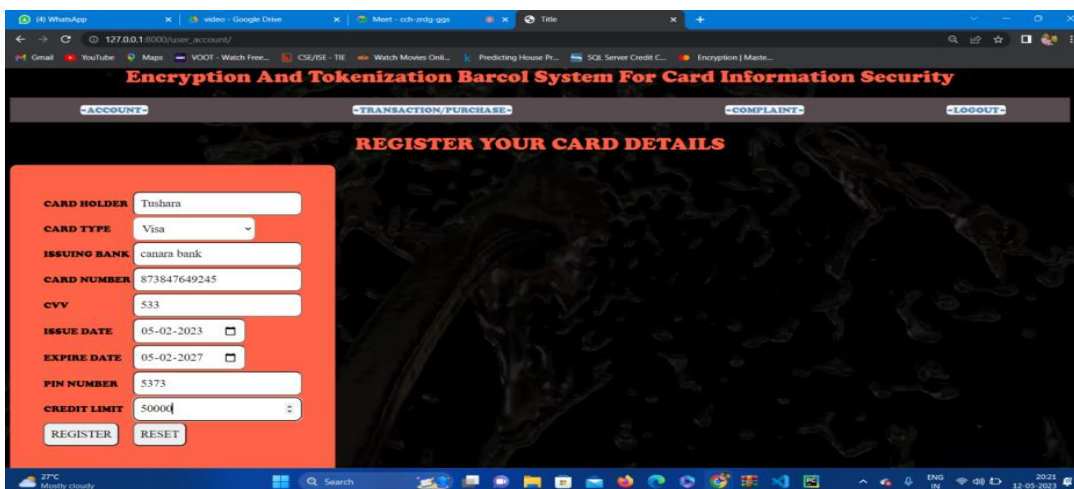
10. Sequence Diagram



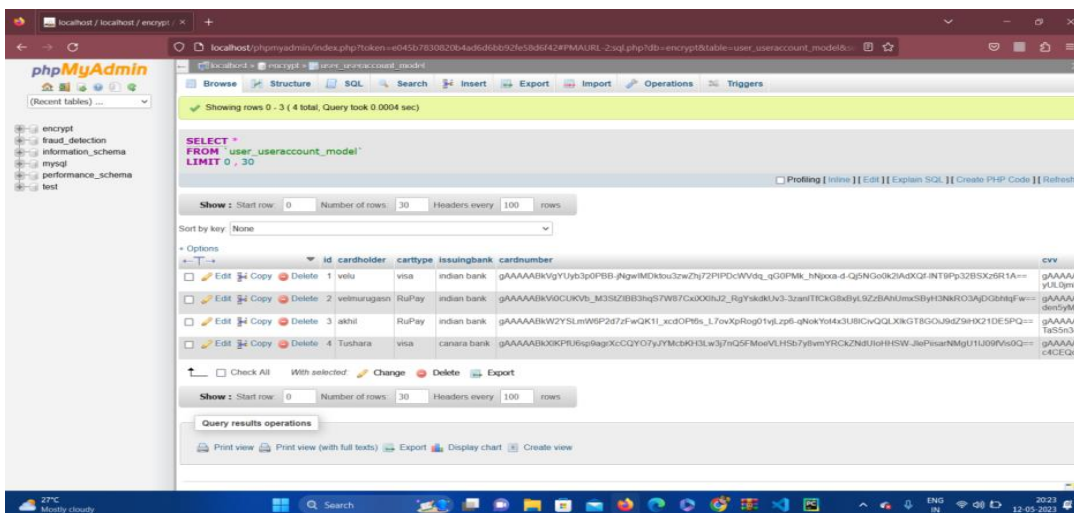
14. User Login



15. Registration Page



16. Encrypted Data



| id | cardholder | cardtype | issuingbank | cardnumber | cvv |
|----|------------|----------|-------------|--|--|
| 1 | velu | visa | indian bank | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== |
| 2 | velmurugan | RuPay | indian bank | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== |
| 3 | akhi | RuPay | indian bank | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== |
| 4 | Tushara | visa | canara bank | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== | gAAAAABKvYUyb3p0F8B_jhgwIMDkx3wZ72PFDcVvdq_g00FMK_hjxxa-d-Q5NGoK2AdXQZiNT9Pp32B5X26R1A== |

12.CONCLUSION

1. We developed the platform to make it simpler to capitalize on the market. We are currently building the site, and one of our main goals is to make it as user-friendly as we can. There is no compelling motivation to press the catch to choose the choice, just as there is no compelling reason to wait for the response.
2. This application combines a language interpretation module, sound-to-information conversion, and voice recognition software. You can have a customer service representative for a variety of organizations, institutions, and fields with a chatbot service provider, or even a receptionist for anyone on the earth. Additionally, chatbots developed on our website will assist you in remembering a variety of products.

13.REFERENCE

- [1] Lekha Athota, Ajay Rana, "Chatbot for Healthcare System Using Artificial Intelligence" Amity University, Noida, June 4-5, 2020, doi:10.1109@ICRITO48877.2020.9197833
- [2] Naing Naing Khin, Khin Mar Soe, "University Chatbot using Artificial Intelligence Markup Language", University of Computer Studies, Yangon, Myanmar, July 2020
- [3] T. Nadarzynski and colleagues, "Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study", Digital Health, vol. 5, pp. 1, January 2019.
- [4] L. Athota et al., "Chatbot for Healthcare System Using Artificial Intelligence", International Conference on Reliability Infocom Technologies and Optimisation, June 2020, p. 620.
- [5] M. Virkar, V. Honmane, and S. U. Rao, "Humanising the Chatbot with Semantics-based Natural Language Generation", International Conference on Intelligent Computing and Control Systems, May 2019, p. 893.
- [6] I. Sutskever, O. Vinyals, and W. Zaremba. Recurrent neural network regularisation is described in arXiv preprint arXiv:1409.2329 from 2014.
- [7] R. B. Mathew et al., "Chatbot for Disease Prediction and Treatment Recommendation Using Machine Learning", International Conference on Trends in Electronics and Informatics, October 2019.

[3] Bushra Kidwai and RK Nadesh, "Design and Development of Diagnostic Chabot for supporting Primary Health Care Systems", International Conference on Computational Intelligence and Data Science (ICCIDS 2019) Procedia Computer Science, vol. 167, pp. 75-84, 2020.

[4] S. Ghare et al., Self-Diagnosis Medical Chat-Bot Using Artificial Intelligence, pp. 1, February 2020.

[5] J Seema, S Suman, S R Chirag, G Vinay and D Balakrishna, "Doctor Chatbot- Smart Health Prediction", International Journal of Scientific Research in Science, vol. 8, pp. 751-756, May-June 2021.